REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23-10-2009	FINAL	

4. TITLE AND SUBTITLE
Cyberwarfare and our Allies: The Importance of Theater Security Cooperation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Christopher V. Greene

Paper Advisor : Professor Richard Crowell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The cyber attacks on the countries of Estonia and Georgia have galvanized the realization that state and non-state actors will exploit vulnerabilities in the information environment to influence national leadership and their critical command and control capabilities. This has serious implications across the globe, and specifically within the U.S. European Command (EUCOM) area of operations. Russia's future use, either state sponsored or through proxies, of cyber attacks to influence NATO Allied domestic decisions regarding energy, missile defense, and security should be expected. The Commander, U.S. EUCOM, is faced with a complex issue, which has the potential to threaten all instruments of national power. This paper will apply the elements of operational art, specifically operational factors and functions, to illustrate why EUCOM must integrate combating cyberwarfare in its theater security cooperation efforts to better prepare NATO Allies for a cyber attack. It delves into the complexity of the cyberwarfare security issue and identifies the need to mitigate vulnerabilities before they can be exploited, advocating the need for enhanced security cooperation efforts. Finally, the paper provides a recommended security cooperation framework to establish priority and unity of effort across the many disparate organizations involved in addressing this complex security issue.

15. SUBJECT TERMS
Cyberwarfare; Theater Security Cooperation; EUCOM; NATO

16. SECURITY CLASSIFICATION OF			**17. LIMITATION**	**18. NUMBER**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		22	401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

Cyberwarfare and Our Allies: The Importance of Theater Security Cooperation

by

Christopher V. Greene

Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

23 Oct 2009

Contents

Abstract

The cyber attacks on the countries of Estonia and Georgia have galvanized the realization that state and non-state actors will exploit vulnerabilities in the information environment to influence national leadership and their critical command and control capabilities. This has serious implications across the globe, and specifically within the U.S. European Command (EUCOM) area of operations. Russia's future use, either state sponsored or through proxies, of cyber attacks to influence NATO Allied domestic decisions regarding energy, missile defense, and security should be expected. The Commander, U.S. EUCOM, is faced with a complex issue, which has the potential to threaten all instruments of national power. This paper will apply the elements of operational art, specifically operational factors and functions, to illustrate why EUCOM must integrate combating cyberwarfare in its theater security cooperation efforts to better prepare NATO Allies for a cyber attack. It delves into the complexity of the cyberwarfare security issue and identifies the need to mitigate vulnerabilities before they can be exploited, advocating the need for enhanced security cooperation efforts. Finally, the paper provides a recommended security cooperation framework to establish priority and unity of effort across the many disparate organizations involved in addressing this security issue.

Introduction

> **"The [cyber] attacks, although not technically very complex, were of great significance, for several reasons…they were intended to create social unrest in response to the domestic policies of a democratically elected government…they were clearly organized…and evidence exists to suggest that the attacks may have been partially state-sponsored.**
>
> **What is perhaps most significant about the recent attacks are the issues they raise and the weaknesses they expose. These are no longer matters of theoretical abstractions, but real life issues that urgently require answers and action."**
>
> **Cyber Conference Opening remarks by Estonian President Ilves, Sep 2009[1]**

In 2007 the country of Estonia was confronted with a wave of cyber attacks, which caused state-wide panic and interruption to critical national services such as banking and media.[2] The attacks were executed using a relatively unsophisticated denial-of-service technique designed to degrade or shut down computer systems or servers by overloading them with simultaneous traffic from thousands of computers.[3] The initial cyber attacks coincided with a domestic debate regarding the removal of a Soviet WWII statue from Estonia's capital city of Tallinn.[4] Estonia blamed the Russian government, but no hard evidence was found to verify their suspicions.[5]

Then in Aug 2008, the country of Georgia was overwhelmed with similar denial-of-service attacks, effectively shutting down government web sites, banks, and media outlets. Alarming was the timing of these attacks, which closely preceded the movement of Russian troops into the disputed region of South Ossetia.[6] Once again, the Russian government was blamed, but at the time, there was little evidence to support such claims. Subsequent analysis suggests the attacks in both Estonia and Georgia, although not completely state-sponsored, may have partially been supported and coordinated by elements of the Russian government.[7]

The significance of these two attacks is not only their evident coordination and potential state-sponsorship, but more importantly the use of cyber attacks to influence

domestic policy and national leadership. This has serious implications across the globe, and specifically within the U.S. European Command (EUCOM) area of operations. Russia's future use, either state sponsored or through proxies, of cyber attacks to influence NATO Allied domestic decisions regarding energy, missile defense, and security, should be expected. President Ilves' warning rings loud, "…these are no longer matters of theoretical abstractions, but real life issues that urgently require answers and action."[8]

"Answers and action" will require the efforts of many across the spectrum of diplomatic, informational, military, and economic instruments of national power. The scope of this paper, however, will focus on the Geographic Combatant Commander's (CCDR), specifically EUCOM's, role in preparing for a cyber attack…not against itself, but against one of its NATO partners. What can be done now to better prepare NATO for a future cyber attack? EUCOM must integrate combating cyberwarfare in its theater security cooperation efforts to better prepare NATO Allies for a cyber attack. The impact of applying security cooperation efforts and mitigating cyber vulnerabilities *before* an attack takes place creates the potential to significantly reduce an adversary's ability to influence national leadership decision making processes and systems. The thesis will be demonstrated using an operational art framework, specifically applying the elements of operational factors and functions.

Discussion and Analysis

Pretend for a moment you have just been assigned to the operational planning staff at EUCOM Headquarters (EUCOM/J5). The cyber attacks in Estonia and Georgia are still fresh in the Commander's mind, and he is concerned. Energy, missile defense, and other security issues continue to irritate NATO-Russian relations, and he has no doubt cyber

attacks will be used in the future to influence these friction points. So what do we do—how do we prepare now for this eventuality? This scenario is very characteristic of the complex challenges facing our Combatant Commanders and their staffs. An operational art framework can help scope these challenges, enabling the development of potential solutions.

Operational art can best be thought of as, "…a bridge and as an interface between strategy and tactics.", and is truly an art as well as a science.[9] It's the Commander's process of visualizing the integration of objectives, resources, sequencing of actions, and risk to accomplish a mission.[10] This is an important framework because today's challenges often span the entire range of military operations and requires cooperation with multiple agencies and national partners. Applying the elements of operational art, specifically operational factors and functions, is an important enabler to tackling the complex challenge of cyberwarfare.

Dr. Milan Vego, in his book *Joint Operational Warfare: Theory and Practice,* defines operational factors as space, time, and force:[11]

Space: Factor space encompasses land, sea, and air (physical environment) as well as human-space, which includes elements such as the political system/leadership, population size and density, economic activity, and technology.[12] Of particular interest is the information space, or what Joint-Pub 3-13 defines as the information environment (IE): the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[13] A quick analysis of the IE in Europe, specifically NATO members in Eastern Europe, reveals an IE that is quite large and complex. Although not exhaustive, it includes computers, the internet, government web sites, banking, cell phones, military

command and control (C2), power grids, control of treatment facilities (water/sewer), transportation, and national/military leaders.

The cyber *attackers* unfortunately are working through the same IE, utilizing many of the same components: internet, power grid, and computers; and not necessarily all from the same location. The attacks on Estonia were assessed to have been initiated by only a few adversaries, but they were able to coordinate attacks by utilizing various social networking tools and infiltrating thousands of computers from around the world.[14]

Time: Factor time includes all aspects of planning, preparing and executing an operation.[15] Vego states that, "Mastering the factor of time…essentially means acting faster than the opponent."[16] In just 2 days, the synchronized cyber attacks basically blockaded the Georgian Government's use of the internet and its ability to communicate with its population.[17] The simplistic nature of the attack, using a denial-of-service technique, meant the attacks were most likely planned and executed in a very short time frame, and at a time of the adversary's choosing (timing). As mentioned earlier, the cyber attacks on Georgia quickly preceded the movement of Russian troops into the disputed region of South Ossetia. Did the cyber attacks affect Georgia's ability to execute C2 between national and military leaders to respond to Russian troop movements? The literature does not indicate any specific degradation in Georgia's C2 capability, but the potential was certainly there.

Force: Vego defines factor force as the, "…military and nonmilitary sources of power employed in support of a particular campaign or major operation."[18] Focusing on the information environment, the adversarial force was small in number, required little sophistication, and was impossible to positively identify. The cyber attacks on Georgia were ultimately assessed to have originated from 10 web sites in Russia and Turkey, registered

with credit cards stolen from U.S. Citizens.[19] A tie to Russian state-sponsorship is perceived, but could not be proven. In addition, the resources needed were minimal; a computer and an internet connection; an extremely low-budget operation, assessed to cost only 4 cents per compromised computer.[20] Bill Woodcock, from Packet Clearing House who works with internet traffic and network development issues, put it into perspective when he stated, "You could fund an entire cyber warfare operation for the cost of replacing a tank tread, so you would be foolish not to."[21] The use of proxies (hackers, criminals, etc.) will make early identification of state-sponsorship almost impossible.

The element of operational factors (space, time, force) bounds the problem and reinforces that cyberwarfare is a complex security issue, having the potential to affect not only military, but all instruments of national power. If operational factors help *frame* the problem, the element of operational functions will help *scope* the problem.

Joint Pub 3-0 defines operational functions as, "…related capabilities and activities grouped together to help JFCs [Joint Force Commanders] integrate, synchronize, and direct joint operations", and includes five basic categories: Command and Control (C2), Intelligence, Fires, Movement and Maneuver, and Protection.[22] Although not exhaustive, these functions represent many of the critical capabilities needed for a joint force to meet its strategic and operational objectives. The functions clearly have a military focus, but some of them also apply to the critical capabilities needed to operate within the other instruments of national power (diplomatic, informational, and economic), specifically functions such as C2, intelligence, and protection. The goal is not to force military doctrine onto a civilian-military problem, but rather to use the doctrinal concept of operational functions to help scope a complex issue.

This research paper will only focus on preserving an Ally's C2 function in the event of a cyber attack. The primary target of the Estonia/Georgia cyber attacks appears to be the national leadership and their ability to effectively govern during a crisis—in essence their ability to command and control (C2). In any EUCOM response to a cyber attack on NATO, preserving the Allies' civilian and military C2 functions will be absolutely critical, whether it involves coordinating the movement of military forces, securing financial transactions, or cooperating in consequence management activities.

The Estonia/Georgia attacks reinforce that efforts to establish a defendable infrastructure to preserve C2 capability, within and amongst the NATO Allies, will be required *before* a cyber attack takes place. This suggests the need for security cooperation activities. Joint Publication (JP) 5-0, *Joint Operation Planning*, defines security cooperation as "…the means by which the Department of Defense (DOD) encourages and enables countries and organizations to work with us to achieve strategic objectives…which serve mutual security interests and build defense partnerships."[23] The goal is to reduce mutual security risks before they can be exploited. JP 5-0 goes on to state that successful security cooperation planning requires, "…close coordination with US agencies that represent other instruments of national power, and particularly with the U.S. chiefs of mission (ambassadors) in the GCCs' AORs."[24]

Proper interagency coordination will be vital to addressing Allied C2 cyber-related vulnerabilities. Although not exhaustive, the following is a list of key players, which should play a role in combating cyberwarfare within the EUCOM theater:

1) ***Host Nation:*** The primary U.S. link to any host nation, including NATO members, is the U.S. Country Team. The team is led by an Ambassador and includes military

personnel such as the Defense Attaché and a Security Assistance Organization (referred to as the Office of Defense Cooperation (ODC) in EUCOM).[25] The Ambassador integrates U.S. foreign policy objectives and resourcing strategies with security assistance needs of the host nation through a Mission Strategic Plan (MSP). The U.S. Country team would be a key player in helping to assess, prioritize, and fund solutions to any host nation C2 vulnerabilities.

2) ***Interagency:*** As noted earlier, because critical national-level C2 capabilities span across all instruments of national power, the inclusion of specific interagency partners will prove essential. To name just a few, representatives from the Department of Treasury may be helpful in identifying C2 vulnerabilities associated with economic processes and institutions; the Department of Energy may be able to advise on energy control vulnerabilities; and the Department of Homeland Security and the Federal Emergency Management Agency (FEMA) may be able to assess emergency response C2 security issues. Fortunately the Geographic Combatant Commanders, including EUCOM, have a Joint Interagency Coordination Group (JIACG), which is an interagency staff group intended to provide collaborative working relationships between civilian and military operational planners.[26]

3) ***NATO:*** In May 2008, almost a year after the attacks in Estonia, NATO established the Cooperative Cyber Defense Center of Excellence (CCD-COE), "…with the aim of enhancing cooperative cyber defence capabilities of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence".[27] The center is not a military unit executing defensive cyber operations, but rather an advisory group that provides cyber defense expertise to partner nations. [28] U.S. security

cooperation planning efforts should include liaison with NATO's CCD-COE to maximize cyber defense expertise specific to the EUCOM theater of operations.

4) ***USCYBERCOMMAND:*** The U.S. understands its increasing dependence on cyberspace as well as the associated risks and vulnerabilities this dependence places on our national security. On 23 June, 2009, the Secretary of Defense directed the Commander, U.S. Strategic Command to establish a subordinate unified command, called U.S. Cyber Command (USCYBERCOM) with primary responsibility to "…secure freedom of action in cyberspace," and capable of "…synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners".[29] Regardless of the specific supported/supporting relationships still being formalized, USCYBERCOMMAND has expertise, which will need to be utilized in order to effectively assess Allied C2 vulnerabilities.

5) ***EUCOM & Security Cooperation:*** EUCOM integrates its security cooperation efforts through the USEUCOM Theater Campaign Plan and associated regional/functional campaign plans. The strategy looks out five years with a focus on proactive engagement, reinforces the need to influence the security environment during peacetime, and recognizes that success depends on interaction with the interagency and aligning actions with those of the host nation.[30] The plan is currently broken down into three regional and two functional campaign plans (figure 1).

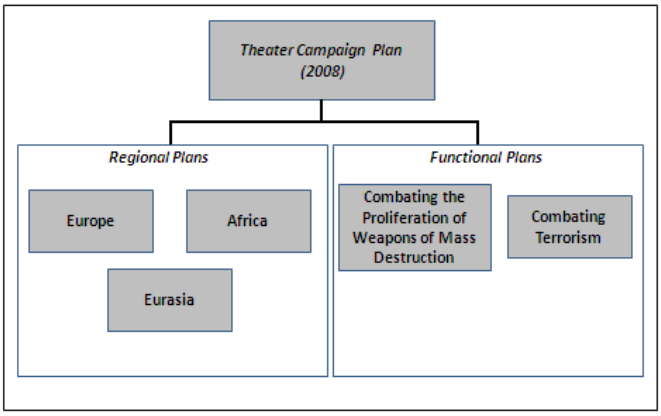

Figure 1: Current U.S. EUCOM Theater Campaign Plan Layout

The current EUCOM Theater Campaign Plan (2008) and associated regional/functional plans make no specific mention of cyberwarfare as a threat or the need to enhance Allied security capabilities in this area. This is not to say EUCOM has not taken any steps to tackle the issue. As part of EUCOM's State Partnership Program, the 175th Network Warfare Squadron from the State of Maryland's National Guard is scheduled to conduct a familiarization visit with Estonian military components later this year, with the goal of identifying specific cyber vulnerabilities.[31] Certainly a move in the right direction, but currently only funded as a military-to-military exchange.

In addition, EUCOM hosts an annual communications exercise called COMBINED ENDEAVOR (CE), which involves US, NATO, and other partner nations. The intent of CE is to facilitate communication integration.[32] Although not specifically focused on combating cyberwarfare against our Allies, CE could be used as a vehicle to assess vulnerabilities and to test potential counter-cyberwarfare processes and procedures.

There is a potential counterargument, though, to EUCOM taking the lead on the cyberwarfare security issue. Some may argue cyberwarfare is a country specific problem or an interagency problem that requires a U.S. Country Team or JIACG-lead versus a military-lead. At a minimum, they may argue USCYBERCOMMAND is the supported commander, and EUCOM needs to wait and see what guidance they give.[33] All valid arguments, but the reality is EUCOM staff may be the only ones with the specific knowledge and capability to provide a theater-wide, disciplined approach to addressing this complex security issue.

The U.S. Country Teams will be a critical part of any planning group, but their focus is country-specific, not intended or capable of planning for a broader theater approach. The JIACG will also provide valuable insight and reach back, but they are not staffed nor trained

to lead a large planning effort. And true, USCYBERCOMMAND is designated the "supported" commander and will most likely be utilized to assist in assessing critical Allied C2 capabilities, however, it can be assumed the Geographic Combatant Commanders will be required to develop a supporting plan, specific to their respective theater of operations.

There is also a NATO treaty obligation, which strongly supports EUCOM involvement and leadership in addressing the cyberwarfare security issue. Article 5 of the NATO Charter basically states an armed attack against one Ally is an attack against them all, and each will assist as required to restore and maintain security.[34] There was debate during the cyber attacks on Estonia as to whether or not to invoke Article 5.[35] It ultimately was not, for various reasons beyond the scope of this paper, but it does highlight the obligation EUCOM has to be *prepared* to respond, either as a supported or supporting command.

The "Who's in charge?" debate should not focus on whose functional lane this falls in, realizing the response to cyberwarfare is not the responsibility of any one department or agency, but rather requires a horizontal approach.[36] The goal should be to designate an organization with the capability to integrate these horizontal efforts into a cohesive and united plan of action.

Analytical Conclusions

The research has revealed three major conclusions: 1) cyberwarfare is a complex security problem with the potential to target all instruments of Allied national power; 2) mitigating critical Allied C2 cyber vulnerabilities requires an integrated effort from numerous civilian and military organizations; and 3) the EUCOM Theater Campaign Plan may be the only instrument currently in existence that can integrate and prioritize funding for efforts amongst these various disparate organizations.

Cyberwarfare is a complex security problem, which can influence all instruments of Allied national power. Combining the operational factors of space, time, and force, EUCOM faces an adversary small in size and extremely difficult, if not impossible to identify. The enemy utilizes easily accessible and low-cost resources (computer, internet, social sites, etc.) and attacks at a time of their choosing; potentially in coordination with other instruments of national power. It does so with relative ease, attacking an Ally's information environment, which spans across diplomatic, informational, economic, and military instruments of national power potentially disrupting anything from cell phones and power grids to national-level C2 systems.

The combined elements of operational factors and functions enabled the transformation of a very complex problem into one that could potentially be solved. This brought to the forefront a very crucial question—solved by whom? Who would be involved and take the lead in tackling this issue that spans all instruments of national power? The reality is EUCOM may be the only entity with the specific theater knowledge and planning capability required to develop a holistic and integrated approach to this security issue. Further, EUCOM's ability to respond *after* a cyber attack is very limited due to the decentralized and unidentifiable structure of most adversarial networks. The key is to reduce Allied cyber-related vulnerabilities *before* they can be exploited. Although not exhaustive, the research identified some of the key players required to develop a theater-wide approach to mitigating critical Allied C2 cyber vulnerabilities. Those organizations included U.S. Country Teams, the interagency represented through the JIACG, the NATO Cyber Defense Center of Excellence, and USCYBERCOMMAND. The combined effort from these various organizations, however, needs to be integrated in an overarching plan.

The EUCOM Theater Campaign Plan may be the only instrument currently in existence, which can integrate efforts and prioritize funding for host nation, interagency, and military security cooperation efforts. The strategy has a long-term planning horizon (5 years) and recognizes the importance of interagency coordination and aligning actions with those of the host nation. The strategy is intended to align foreign assistance, exercises, military engagements, and US Country Team Mission Strategic Plans to meet overall security objectives in the host nation as well as the region. The current strategy, though, does not have a functional plan dedicated to combating cyberwarfare across the EUCOM area of operations like it does for combating terrorism and the proliferation of weapons of mass destruction.

Recommendation:

EUCOM should modify its existing Theater Campaign Plan to include an additional functional plan…*Combating Cyberwarfare* (figure 2). Although progress has been and continues to be made to protect U.S. cyber vulnerabilities, the focus of this functional plan is security cooperation activities to mitigate NATO Allied cyber vulnerabilities. Developing a new functional plan to combat cyberwarfare establishes it as a priority, recognizes cyberwarfare as an "inter-state" versus "intra-state" problem, and establishes the framework to enable the unity of effort required to reduce vulnerabilities *before* they can be exploited.

First, the collective efforts from across the interagency are required to tackle this security issue. Communicating the commander's priority to address these vulnerabilities is absolutely critical to acquiring the requisite participation from disparate planning staffs, as well as securing funding for any potential security cooperation efforts.

Second, developing a functional vs. regional plan emphasizes the theater-wide scope of this security issue rather than the isolated threat to any one country. The information environment, which for example facilitates the control of power grids, telecommunications, and commerce has no state boundaries, but is rather *inter*-connected. An adversary's ability to exploit a weak information link in one country has the potential to impact the cyber domain across the entire theater. A functional plan will provide a holistic approach to assessing and reducing cyber vulnerabilities across the EUCOM area of responsibility.

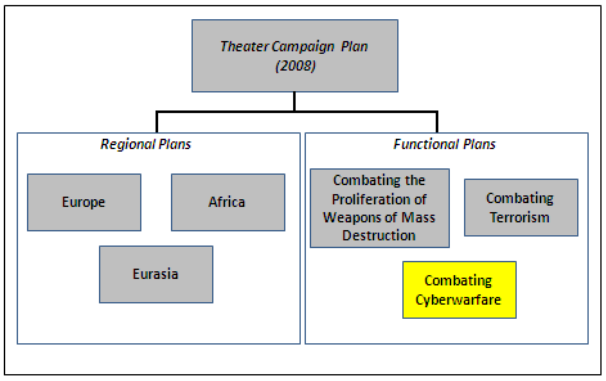

Figure 2: Recommended U.S. EUCOM Theater Campaign Plan Layout

Lastly, developing a new *Combating Cyberwarfare Functional Plan* provides the necessary security cooperation framework required to establish at least some level of unity of effort across not only US, but NATO and host nation organizations. Positive actions have been taken since the cyber attacks on Estonia and Georgia including the establishment of NATO's Cooperative Cyber Defense Center of Excellence and the Maryland-Estonia familiarization visit scheduled for late 2009. But there is no indication these efforts have been linked or integrated. The new functional plan would provide the framework needed to integrate efforts like these to ensure the most efficient use of scarce resources.

Complete unity of effort is probably not achievable considering the information environment is massive and resides largely in the private sector where there is sensitivity to revealing cyber network schematics, if even available, and vulnerabilities. Considering this reality, the initial functional plan should specifically focus on critical vulnerabilities to key

government-led command and control networks and their critical links to the private sector. Success in this one functional area may provide the trust and momentum to focus on additional critical national functions in the future.

Given that EUCOM/J5 has primary responsibility for developing the EUCOM Theater Campaign Plan, the J5 should also take the lead in developing a new *Combating Cyberwarfare Functional Plan*. A Combating Cyberwarfare Planning Group (CCPG) should be established to formalize the process and to communicate the commander's intent and priority. The CCPG, led by the J5, should include typical J-staff representatives to include but not limited to intelligence, operations, communications, comptroller, and should also include representatives from the JIACG to utilize interagency expertise, USCYBERCOMMAND to link global counter-cyberwarfare planning efforts and funding, U.S. Country Teams to establish links with host nation functions and ensure integration with Mission Strategic Plans, and finally NATO's Cyber Defense Center of Excellence to collaborate on NATO/European efforts.

Conclusion

The cyber attacks on Estonia and Georgia have galvanized the realization that state and non-state actors will exploit vulnerabilities in the information environment to influence national leaders and their critical command and control capabilities. Combatant Commanders, including the Commander of U.S. European Command, are now faced with this complex security issue. With serious NATO-Russian friction points over energy, missile defense, and security, future cyber attacks against our Allies can be expected. EUCOM must integrate combating cyberwarfare in its theater security cooperation efforts before an attack occurs to better prepare NATO Allies against future cyber attacks.

The research has revealed that first, cyberwarfare is a very complex security problem, with the potential to influence all instruments of allied national power. However, the application of the elements of operational art, specifically operational factors and functions, demonstrate the potential to frame and scope this complex security issue into a workable solution. Second, addressing the cyberwarfare security issue requires the involvement of numerous organizations across both military and civilian sectors. Even though some progress has been made to reduce cyber vulnerabilities and enhance cyber defense capabilities, there is no overarching plan establishing unity of effort to combat cyberwarfare. Lastly, the EUCOM Theater Campaign Plan may be the only vehicle currently in existence, which can integrate and prioritize funding for host nation, interagency, and military efforts to combat cyberwarfare.

In lieu of these conclusions, the recommendation is to modify the existing EUCOM Theater Campaign Plan to include an additional functional plan…*Combating Cyberwarfare,* focused on security cooperation activities to mitigate Allied C2 cyber-related vulnerabilities. Developing a new functional plan to combat cyberwarfare establishes the effort as a priority, recognizes cyberwarfare as an "inter-state" versus "intra-state" problem, and provides the framework to enable the unity of effort required to address vulnerabilities *before* they can be exploited.

End Notes

[1] Sarabjit Jagirdar, "ESTONIA: President Ilves Speaks on Occasion of International Cyber Conflict Legal, Policy conference in Tallinn," *US Federal News Service*, 11 September 2009, http://proquest.umi.com/pqdweb?did=1857360081&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 September 2009).
[2] Henry S. Kenyon, "Cyber Attacks Reveal Lessons," *Signal*, July 2009, http://proquest.umi.com/pqdweb?did=1798841591&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 17 Oct 2009).
[3] Distributed Denial-of-Service (DDoS) Attack: A means of burdening or effectively shutting down a remote system by bombarding it with traffic from many other computers. DDoS attacks are often launched using the compromised systems of Internet users, often using botnets. An attacker will exploit a vulnerability in one computer system and make it the DDoS "master" using *Remote Control Software*. Later, the intruder will use the master system to identify and manage zombies that can perform the attack, http://www.antispywarecoalition.org/documents/GlossaryJune292006.htm.
[4] Henry S. Kenyon, "Cyber Attacks Reveal Lessons," *Signal*, July 2009, http://proquest.umi.com/pqdweb?did=1798841591&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 17 Oct 2009).
[5] Breanne Wagner, "Cyber Attacks in Estonia Serve as Wake-Up Call," *National Defense Industrial Association,* October 2007, http://proquest.umi.com/pqdweb?did=1367884241&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 Sep 2009).
[6] Joshua E. Kastenberg and Stephen W. Korns, "Georgia's Cyber Left Hook," *Parameters,* Winter 2008/2009, http://proquest.umi.com/pqdweb?did=1663729531&sid=3&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 September 2009).
[7] David A. Fulghum, "Network Threats Evolving, Growing More Dangerous," *Aerospace Daily and Defense Report,* 21 August 2009, http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do (accessed 16 October 2009).
[8] Sarabjit Jagirdar, "ESTONIA: President Ilves Speaks on Occasion of International Cyber Conflict Legal, Policy conference in Tallinn," *US Federal News Service*, 11 September 2009, http://proquest.umi.com/pqdweb?did=1857360081&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 September 2009).
[9] Dr. Milan Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2009), I-3.
[10] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Operation Planning*. Joint Publication 5-0, (Washington, DC: CJCS, 26 December 2006, IV-1.
[11] Ibid, III-3.
[12] Ibid, III-7.
[13] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Information Operations.* Joint Publication 3-13, (Washington, DC: CJCS, 13 February 2006), x.
[14] David A. Fulghum, "Network Threats Evolving, Growing More Dangerous," *Aerospace Daily and Defense Report,* 21 August 2009, http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do (accessed 16 October 2009).
[15] Dr. Milan Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2009), III-19.
[16] Ibid, III-19.
[17] Joshua E. Kastenberg and Stephen W. Korns, "Georgia's Cyber Left Hook," *Parameters,* Winter 2008/2009, http://proquest.umi.com/pqdweb?did=1663729531&sid=3&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 September 2009).
[18] Dr. Milan Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2009), III-33.

[19] David A. Fulghum, "Network Threats Evolving, Growing More Dangerous," *Aerospace Daily and Defense Report,* 21 August 2009, http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do (accessed 16 October 2009).
[20] Elizabeth H. Manning, "Lessons Learned from the First War Fought in Cyberspace," *The Officer,* Feb/Mar 2009, http://proquest.umi.com/pqdweb?did=1701692761&sid=2&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 19 September 2009).
[21] Ibid.
[22] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Operations.* Joint Publication 3-0, (Washington, DC: CJCS, 13 February 2008), III-1.
[23] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Operation Planning*. Joint Publication 5-0, (Washington, DC: CJCS, 26 December 2006, I-3.
[24] Ibid.
[25] U.S. Office of the Chairman of the Joint Chiefs of Staff, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I.* Joint Publication 3-08, (Washington, DC: CJCS, 17 March 2006), II-17 to II-19.
[26]Ibid, xii.
[27] Wire feed, "Cyber Defence Centre of Excellence Receives Accreditation"**,** *US Federal News Service*, 13 November 2008, http://proquest.umi.com/pqdweb?index=0&did=1596194931&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1255980917&clientId=18762 (accessed 19 Oct 2009).
[28] Newswire, "NATO Center of Excellence in Cyber Defense to be set up in Estonia," *Baltic News Service*, 11 February 2008, http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T7634620058&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T7634620062&cisb=22_T7634620061&treeMax=true&treeWidth=0&csi=172030&docNo=3 (accessed 19 Oct 2009)
[29] Robert M. Gates, U.S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, June 23, 2009.
[30] U.S. European Command, *Headquarters, USEUCOM Theater Campaign Plan.* (Stuttgart, Germany: EUCOM, 4 June 2008).
[31] Lt Col Weidanz, Roy. Phone interview. 25 September 2009.
[32] Stacy Fowler, "Opening Ceremony Kicks off Combined Endeavor 2008," *U.S. Air Forces in Europe News Service*, 7 May 2008, http://proquest.umi.com/pqdweb?did=1484240281&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 5 Oct 2009).
[33] Robert M. Gates, U.S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, 23 June 2009.
[34] North Atlantic Treaty Organization, "North Atlantic Treaty Charter," 4 April 1949, http://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed 17 October 2009).
[35] Henry S. Kenyon, "Cyber Attacks Reveal Lessons," *Signal*, July 2009, http://proquest.umi.com/pqdweb?did=1798841591&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 17 Oct 2009).
[36] Ibid.

Bibliography

Fowler, Stacy. "Opening Ceremony Kicks off Combined Endeavor 2008." *U.S. Air Forces in Europe News Service,* 7 May 2008. http://proquest.umi.com/pqdweb?did=1484240281&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 5 Oct 2009).

Fulghum, David A. "Network Threats Evolving, Growing More Dangerous." *Aerospace Daily and Defense Report,* 21 August 2009. http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do (accessed 16 October 2009).

Gates, Robert M., U.S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." 23 June 2009.

Jagirdar, Sarabjit. "ESTONIA: President Ilves Speaks on Occasion of International Cyber Conflict Legal, Policy conference in Tallinn." *US Federal News Service*, 11 September 2009. http://proquest.umi.com/pqdweb?did=1857360081&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 September 2009).

Kastenberg, Joshua E. "Georgia's Cyber Left Hook." *Parameter,* Winter 2008/2009. http://proquest.umi.com/pqdweb?did=1663729531&sid=3&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 September 2009).

Kenyon, Henry S. "Cyber Attacks Reveal Lessons." *Signal*, July 2009. http://proquest.umi.com/pqdweb?did=1798841591&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 17 Oct 2009).

Manning, Elizabeth H. "Lessons Learned from the First War Fought in Cyberspace." *The Officer,* Feb/Mar 2009. http://proquest.umi.com/pqdweb?did=1701692761&sid=2&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 19 September 2009).

North Atlantic Treaty Organization. "North Atlantic Treaty Charter." 4 April 1949. http://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed 17 October 2009).

U.S. European Command. *Headquarters, USEUCOM Theater Campaign Plan.* Stuttgart, Germany: EUCOM, 2008.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations.* Joint Publication 3-0, Washington, DC: CJCS, 13 February 2008.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I.* Joint Publication 3-08, Washington, DC: CJCS, 17 March 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations.* Joint Publication 3-13, Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operation Planning*. Joint Publication 5-0, Washington, DC: CJCS, 26 December 2006.

Vego, Milan. *Joint Operational Warfare: Theory and Practice.* Newport, RI: Naval War College, 2009.

Wagner, Breanne. "Cyber Attacks in Estonia Serve as Wake-Up Call." *National Defense Industrial Association,* October 2007. http://proquest.umi.com/pqdweb?did=1367884241&sid=1&Fmt=3&clientId=18762&RQT=309&VName=PQD (accessed 18 Sep 2009).